UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

BITSIGHT TECHNOLOGIES, INC., Plaintiff, v. NORMSHIELD INC. d/b/a BLACK KITE INC., Defendant.	)	Civil Action No. 23-cv-12055-MJJ

MEMORANDUM AND ORDER ON DEFENDANT'S MOTION TO DISMISS

September 20, 2024

JOUN, D.J.

BitSight Technologies, Inc. ("BitSight") brings suit against NormShield, Inc. d/b/a Black Kite ("Black Kite") alleging infringement of its patents, U.S. Patent Nos. 9,438,615 (the "'615 patent"); 9,973,524 (the "'524 patent"); 10,805,331 (the "'331 patent"); 11,652,834 (the "'834 patent"); and 11,777,976 (the "'976 patent") (collectively, the "Asserted Patents"). [Doc. No. 39]. Additionally, BitSight brings claims of false advertising under 15 U.S.C. § 1125(a) (the "Lanham Act") and M.G.L. c. 266, as well as for deceptive trade practices under M.G.L. c. 93A, § 11. [*Id.*]. Black Kite moves to dismiss the First Amended Complaint (the "FAC") on the grounds that the Asserted Patents are directed to patent-ineligible abstract ideas under 35 U.S.C. § 101, and BitSight's false advertising claims are insufficient as a matter of law. [Doc. No. 45]. For the following reasons, Black Kite's motion is GRANTED in part and DENIED in part.

I. BACKGROUND

A. Overview

BitSight is a Delaware corporation based in Massachusetts. [Doc. No. 39 at ¶ 10]. It was founded in 2011. [*Id*. at ¶ 2]. BitSight developed a system for determining a composite security rating—a universal metric to interpret cyber risk—for a third-party entity, derived by amassing security data collected externally from third-party computer systems online and resulting in a proprietary data set of security related events, assets, and effects. [*Id*. at ¶ 17]. This system enables BitSight to assess an entity's security risk without access to the entity's internal documents and systems, and it can also optionally process additional, user-provided information regarding the entity and its IP assets. [*Id*. at ¶¶ 18-19]. Similar to a credit score, BitSight issues Security Ratings ranging in value from 250 to 900. [*Id*. at ¶ 20]. BitSight has incorporated its technology and data models in several product offerings. [*Id*. at ¶ 24]. Prior to the development of BitSight's technology, cybersecurity assessments of third parties (including through relying on publicly available information) existed, but they were slow, expensive, impractical, and applied haphazardly such that they failed to consistently predict the actual performance of a company's security program. [*Id*. at ¶¶ 15-16, 34, 66].

Black Kite is a Delaware corporation based in Massachusetts. [*Id*. at ¶ 11]. It was founded in 2016. [*Id*. at ¶ 7]. Black Kite purports to have also developed a platform that can provide cybersecurity assessments of third parties, relying on publicly accessible, external data. [*Id*. at ¶¶ 82-83, 85]. Black Kite's platform communicates its findings by arriving at a score, which it calls a "Cyber Risk Score," issued as a letter-grade. [*Id*. at ¶ 89].

B. The Asserted Patents

The FAC alleges that Black Kite infringes five patents owned by BitSight: the '331 patent, the '524 patent, the '976 patent, the '615 patent, and the '834 patent. [Doc. No. 39 at ¶ 1]. These patents concern "BitSight's methods and systems underlying its approach to locating, collecting, analyzing, and communicating cyber risk management data." [*Id*. at ¶ 27].

1. *The '331, '524 and '976 Patents*

The '331, '524, and '976 patents share a common specification and claim priority to September 24, 2010. [Doc. No. 39-2 at 2; Doc. No. 39-3 at 2; Doc. No. 39-4 at 2]. These patents relate to "systems for determining the security of information systems and, in particular, for evaluating the security of third-party computer systems." [Doc. No. 39 at ¶ 33]. Specifically, the shared specification of the '331, '524, and '976 patents discloses a method and system "for creating a composite security rating from security characterization data of a third-party computer system" that is "derived from externally observable characteristics of the third-party computer system." [*Id*. at ¶ 37; Doc. No. 39-2 at 12; Doc. No. 39-3 at 8; Doc. No. 39-4 at 14]. The specification further discloses that "[a] diverse set of network sensors and services around the Internet collect and observe information about the third-party entity computer systems. The system then gathers, processes, and stores the data collected about entities from the sensors and service providers using custom developed data source specification collection processors." [Doc. No. 39 at ¶ 37; Doc. No. 39-2 at 15; Doc. No. 39-3 at 11; Doc. No. 39-4 at 17].

The FAC alleges that Black Kite infringes "at least claims 1-3, 8, and 29 of the '331 patent." [Doc. No. 39 at ¶ 123]. Claim 1 recites in full:

> 1. A method comprising:
> collecting information about two or more organizations that have computer systems, network resources, and employees, the organizations posing risks through business relationships of the organizations with other parties, the information

> collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations and indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations, the information indicative of durations of events associated with compromises or vulnerabilities or configurations,
> at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet,
> the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,
> at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names,
> at least one of the sources for each of the organizations comprising a public source or a commercial source,
> processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics,
> the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to the duration of detected malicious activity, and
> in connection with assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering reports of the composite ratings of the organizations through a reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations.

[Doc. No. 39-2 at 19-20]. Claims 2, 3, and 8 depend directly or indirectly on claim 1 and describe the "collected information." [*Id*. at 20]. Claim 2 recites that it "is represented by at least two data types," and claim 3 recites a list of those data types. [*Id*.]. Claim 8 recites that the collected information "indicates whether a computer system of each of the organizations communicated with a known attacker controlled network or sensor outside the control or

network of the organization." [*Id.*]. Claim 29's limitations largely overlap with those of claim 1—e.g., "collecting information" about an organization via the Internet without the organization's permission, "processing the information by computer to form a composite rating of the organization," and "delivering a report of the composite rating of the organization" to a user. [*Id.* at 21].

The FAC alleges infringement of one or more claims of the '524 patent, including claims 1, 6, and 13. [Doc. No. 39 at ¶ 134]. Claim 1 recites in full:

> 1. A computer implemented method comprising:
> on one or more computers, maintaining in a database an entity map that maps technical assets to respective companies or other entities with which the assets are associated, wherein mapping technical assets to respective companies or other entities comprises determining IP information by annotating a domain name with naming conventions for at least one of a mail server, an SMTP server, and an FTP server, thereby deriving a likely server name having assigned IP addresses,
> automatically using [*sic*] sensors on the Internet to collect externally observable cyber-security characterizations of the technical assets that have been mapped to each of the entities and associating the observable cybersecurity characterizations with a respective entity based at least in part on the derived server name,
> automatically deriving observations about the technical assets from the collected cyber-security characterizations, wherein the derived observations comprise (i) a number of technical assets that have been reported to be malicious and (ii) a duration of detected malicious activity associated with the technical assets,
> automatically generating a cyber-security rating for each of the entities using the entity map and the derived observations, and
> through a communication network, exposing to users in a user interface of a portal, information about the cybersecurity ratings of the entities that is useful to decisions about entities with which to do business.

[Doc. No. 39-3 at 15-16]. Claims 6 and 13 depend on claim 1, and respectively recite "maintaining an entity map comprises using a domain name associated with the entity" and "the technical assets comprise ranges of IP addresses." [*Id*. at 16].

The FAC further alleges that Black Kite infringes "at least claim 1 of the '976 patent." [Doc. No. 39 at ¶ 141]. Claim 1 recites in full:

> 1. A method for determining a security rating of an entity, the method comprising:
> determining an internal security rating comprising:

obtaining data indicative of internal security from a plurality of internal data sources;
extracting a plurality of internal security features from the obtained data;
applying a respective transformation function to each of the plurality of internal security features to determine a first plurality of transformed features; and
combining the first plurality of transformed features to form the internal security rating;
determining an external security rating comprising:
obtaining data indicative of external security from a plurality of external data sources;
extracting a plurality of external security features from the obtained data;
applying a respective transformation function to each of the plurality of external security features to determine a second plurality of transformed features; and
combining the second plurality of transformed features to form the external security rating; and
providing, via a reporting facility, a composite security rating for the entity based on the internal security rating and the external security rating, wherein at least one of the internal security features or the external security features indicates malicious activity associated with an IP address of the entity.

[Doc. No. 39-4 at 21-22].

2. *The '615 Patent*

The '615 patent was issued on September 6, 2016. [Doc. No. 39 at ¶ 61]. It describes that the activities of an online user associated with an entity can leave traces, and those traces can be analyzed to infer the security state of the entity and "map an entity's assets that accounts for both publicly available information as well as a user's non-technical information." [*Id*. at ¶ 69; Doc. No. 39-5 at 2].

The FAC alleges infringement of one or more claims of the '615 patent, including claims 84-85 and 87-90. [Doc. No. 39 at ¶ 152]. Claim 84 recites in full:

84. A method comprising:
generating a map between (a) technical assets that contribute to security characteristics of respective entities and (b) the identities of the entities that are associated with the respective technical assets, at least part of the generating of the map being done automatically,
generating graphs of relationships among entities based on their associations with technical assets; and

> enabling a user to assist in the generating of the map by presenting to the user through a user interface (a) data about the technical assets of entities and (b) an interactive tool for associating the technical assets with the identities of the entities.

[Doc. No. 39-5 at 39]. Claims 85 and 87-90 depend directly or indirectly on claim 84. [*Id.*]. Claim 85 recites that the "technical assets comprise network-related information." [*Id.*]. Claims 87 and 88 recite that "generating the map comprises online discovery of information about the technical assets," and that the information "is discovered from an Internet Assigned Numbers Authority or a Regional Internet Registry." [*Id.*]. Finally, claims 89 and 90 recite the use of passive DNS queries to discover information about technical assets. [*Id.*].

3. *The '834 Patent*

The '834 patent was issued on May 16, 2023, as a continuation of the '615 patent. [Doc. No. 39 at ¶¶ 62-63]. The FAC alleges infringement of "at least claim 1 of the '834 patent," which describes a series of back-and-forth DNS queries used to identify a third-party's digital assets via IP addresses. [Doc. No. 39 at ¶¶ 75-76, 159]. Claim 1 recites in full:

> 1. A computer-implemented method for mapping Internet Protocol (IP) addresses to an entity, the method comprising:
> receiving a first domain name for the entity;
> sending, to a domain name system (DNS) server, a first passive DNS query to identify first name servers for the first domain name;
> receiving, from the DNS server, a list of the first name servers for the first domain name;
> sending, for each of the first name servers, a second passive DNS query to identify second domain names for which the first name server is authoritative;
> receiving, for each of the first name servers, a list of the second domain names for which the first name server is authoritative;
> sending, for each of the second domain names, a third passive DNS query to identify host names for the hosts of the second domain name and IP addresses for the host names;
> receiving a list of the host names and the IP addresses for the host names; and
> mapping each IP address to an attribute for the entity.

[Doc. No. 39-6 at 42].

C. Black Kite's Advertising

In addition to its patent infringement claims, BitSight claims Black Kite has made false and misleading statements about BitSight and about Black Kite's own capabilities. [Doc. No. 39 at ¶ 94]. This includes statements published on Black Kite's website, including on the "Black Kite Competitive Comparison" page (hereinafter "Black Kite Comparison"), where Black Kite compares its offerings to those of its competitors. [*Id.*; Doc. No. 39-14]. On that page, Black Kite states that it has 290 controls while BitSight has 40 controls. [Doc. No. 39 at ¶ 96; Doc. No. 39-14 at 2]. Black Kite includes in this count data that does not qualify as "controls," as that term is understood by the industry and defined by the National Institute of Standards and Technology's ("NIST"), which defines a "control" as "[a] safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements." [Doc. No. 39 at ¶ 97]. Black Kite notes on a separate webpage, not referenced in the Black Kite Comparison, that it uses a different definition of "control" to categorize data. [*Id.* at ¶ 98].

The Black Kite Comparison also states that Black Kite has "extensive" seamless integration with RSA Archer, Splunk, OneTrust, and ServiceNow, while BitSight only has "partial" integrations. [*Id.* at ¶ 99; Doc. No. 39-14 at 2]. But BitSight has numerous extensive, pre-built integrations, which specifically include RSA Archer, Splunk, OneTrust, and ServiceNow, as well as others. [Doc. No. 39 at ¶ 100]. Similarly, the Black Kite Comparison states that Black Kite offers "extensive" digital footprint discovery, while BitSight only offers "partial" digital footprint discovery. [*Id.* at ¶ 101]. But BitSight has continuously used both automated and human-curated processes in its digital footprint capability since it was founded,

and has labeled asset data for many companies to use in AI and machine learning models. [*Id*. at ¶¶ 102-03].

The Black Kite Comparison goes on to note that Black Kite can add a new vendor "instant[ly]," but that it takes "days" to add a new vendor using BitSight. [*Id*. at ¶ 104; Doc. No. 39-14 at 3]. The "Days" notation includes a footnote elaborating, "Days if not pre-evaluated. Instant if pre-evaluated." [Doc. No. 39-14 at 5]. However, under Black Kite's license model, adding a new vendor requires a manual request to a customer service agent—such that a new vendor cannot be added instantly. [Doc. No. 39 at ¶ 105]. In contrast, BitSight allows its customers to add new vendors via self-service rather than interacting with a service agent, resulting in a quicker process. [*Id*.].

The Black Kite Comparison further notes that Black Kite has a "RSI™" or "Ransomware Susceptibility Index®," while BitSight does not have one available. [*Id*. at ¶ 106-07; Doc. No. 39-14 at 3]. BitSight does not offer the Ransomware Susceptibility Index®—Black Kite's branded ransomware likelihood indicator—but it does offer its own ransomware likelihood indicator. [Doc. No. 39 at ¶ 107]. And the Black Kite Comparison states that Black Kite has custom questionnaire mapping and can add questionnaires and other security attestations, but that BitSight does not. [*Id*. at ¶¶ 108, 110]. To the contrary, BitSight does map its findings to questions and control sets, and its offerings can have questionnaires and other security attestations added. [*Id*. at ¶¶ 109, 111].

Generally, the Black Kite Comparison uses these various comparison points to claim, "Although each Black Kite competitor has a different approach, Black Kite prides itself on having the highest quality data." [*Id*. at ¶ 115; Doc. No. 39-14 at 5].

II. § 101 CLAIMS

A. Legal Standard

To survive a Rule 12(b)(6) motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to "state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Dismissal may be warranted based on "the inevitable success of an affirmative defense," such as patent invalidity, if "the only plausible reading" of the allegedly infringed patent "is one that demonstrates that the patent claims cover subject matter that is not eligible for patenting." *Riggs Tech. Holdings, LLC v. Cengage Learning, Inc.*, 581 F. Supp. 3d 357, 360 (D. Mass. 2022), *aff'd*, No. 2022-cv-1468, 2023 WL 193162 (Fed. Cir. Jan. 17, 2023) (cleaned up).

Section 101 of the Patent Act provides that "[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor," subject to three subject matter exceptions: "laws of nature, natural phenomena, and abstract ideas." 35 U.S.C. § 101; *Bilski v. Kappos*, 561 U.S. 593, 601 (2010). Such concepts are not patentable. *Bilski*, 561 U.S. at 601. The Supreme Court has devised a two-stage framework to determine whether these exceptions apply. *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014). Under this framework, a court must (1) "determine whether the claims at issue are directed to one of those patent-ineligible concepts" and, if so, (2) "consider the elements of each claim both individually and as an ordered combination to determine whether the additional elements transform the nature of the claim into a patent-eligible application." *Id*. (cleaned up).

Under the first step of the *Alice* framework, the Court "look[s] at the 'focus of the claimed advance over the prior art' to determine if the claim's 'character as a whole' is directed

to excluded subject matter." *Affinity Labs of Texas, LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016) (citations omitted). Regarding computer-related technology, the primary question is "whether the focus of the claims is on the specific asserted improvement in computer capabilities … or, instead, on a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool." *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335–36 (Fed. Cir. 2016); *see also Smart Software, Inc. v. PlanningEdge, LLC*, 192 F. Supp. 3d 243, 250 (D. Mass. 2016) ("courts will . . . look for an improvement to the functioning of the computer itself").

A court need only proceed to *Alice* step two if the claims fail step one. *Alice*, 573 U.S. at 217. At step two, the Court "consider[s] the elements of each claim both individually and as an ordered combination to determine whether the additional elements transform the nature of the claim into a patent-eligible application." *Id*. (cleaned up). The claim elements should "involve more than performance of well-understood, routine, and conventional activities previously known to the industry." *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat. Ass'n*, 776 F.3d 1343, 1347-48 (Fed. Cir. 2014) (cleaned up). They should "include 'additional features' to ensure 'that the [claim] is more than a drafting effort designed to monopolize the [abstract idea].'" *Alice*, 573 U.S. at 221 (quoting *Mayo Collaborative Servs. v. Prometheus Lab'ys, Inc.*, 566 U.S. 66, 77 (2012)). "[A]n inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces." *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016).

B. Analysis

1. The '331, '524 and '976 Patents

i. *Alice* Step One

At stage one of the *Alice* analysis, the claims of the'331, '524 and '976 patents are

directed to a patent-ineligible concept. As detailed above, the shared specification discloses a method and system whereby (1) "network sensors and services around the Internet collect and observe information"; (2) the system "then gathers, processes, and stores the data collected"; and (3) a "composite security rating" is created from this data. [Doc. No. 39 at ¶ 37; Doc. No. 39-2 at 12, 15; Doc. No. 39-3 at 8, 11; Doc. No. 39-4 at 14, 17]. In other words, "[t]he focus of the asserted claims . . . is on collecting information, analyzing it, and displaying certain results of the collection and analysis"—all of which comprise abstract-idea processes, and nothing more. *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1351-53 (Fed. Cir. 2016) (finding abstract idea where patent described (1) "receiving data," (2) "detecting and analyzing events in real-time from the plurality of data streams," and (3) displaying analysis results and "deriving a composite indicator of reliability"); *see also Reputation.com, Inc. v. Birdeye, Inc.*, No. CV 21-129-LPS-CJB, 2022 WL 609161, at *11 (D. Del. Jan. 31, 2022), *adopted* 2022 WL 951408 (D. Del. Mar. 30, 2022) (finding abstract idea of "assessing an individual's reputation based on documents about the individual to generate a reputation score"). Further, as acknowledged by BitSight, the general concept of assessing the cybersecurity risk of third parties is a "fundamental [and] long prevalent" business practice, constituting an abstract idea itself. *Intell. Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1314 (Fed. Cir. 2016) ("The Supreme Court has held that 'fundamental ... practice[s] long prevalent' are abstract ideas." (quoting *Alice*, 573 U.S. at 219)); *see, e.g.*, [Doc. No. 39 at ¶ 34 ("Prior to the invention of the '331,'524, and '976 patents, "[w]hen a company want[ed] to reduce its cyber security risk of doing business with another company's computer systems, it [had to] either perform[], or hire[] an outside firm to perform, a cyber security risk assessment of the other company to determine if it is following good security practices."); Doc. No. 39-2 at 12 (same); Doc. No. 39-3 at 8 (same); Doc. No. 39-4 at 14 (same)].

BitSight argues that these patents are not directed to an abstract concept because "the claimed inventions of the '331, '524, and '976 patents recite non-conventional uses of sensors on the internet to collect externally observable information, without permission of the third-party organization, which provide for more accurate and efficient cybersecurity assessments and solve technological problems left unaddressed by the prior art internal cybersecurity risk assessments." [Doc. No. 49 at 15]. But nothing in this assertion converts the abstract ideas of the '331, '524, and '976 patents into something concrete.

First, the patents' recitation of generic "sensors" does not transform the claims such that they are directed to a patent-eligible idea. While BitSight attempts to analogize this case to *Thales*, the *Thales* patent differed in that it described "an inertial tracking system for tracking the motion of an object" using physical "inertial sensors, such as accelerometers and gyroscopes." *Thales Visionix Inc. v. United States*, 850 F.3d 1343, 1344-45 (2017). Because "[t]he claims specif[ied] a particular configuration of inertial sensors and a particular method of using the raw data from the sensors in order to more accurately calculate . . . an object on a moving platform" rather than merely reciting completely conventional sensors, the Federal Circuit found the claims were not directed to an abstract idea. *Id*. at 1349. Here, in contrast, the specification and asserted claims of the '524 and '331 patents provide no detail on how the non-physical sensors are designed or configured to collect the information sought. *See, e.g.*, Doc. No. 39-2 at 15 (specification describing "[a] diverse set of network sensors and services around the Internet collect and observe information about the third party entity computer systems"); *id*. at 19 (claim 1 reciting "at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet"). The claims "simply claim[] a result and then add[] additional data processing steps without claiming any specific improvement in the

computer technology itself." *Cambridge Mobile Telematics, Inc. v. Zendrive, Inc.*, No. CV 22-1260-RGA, 2023 WL 4850567, at *6 (D. Del. July 28, 2023), *adopted*, 2023 WL 6295338 (D. Del. Sept. 27, 2023). Accordingly, the recitation of sensors is not enough for eligibility.[1]

Second, to the extent that BitSight argues for a non-abstract concept based on the patents' focus on collecting externally observable data (as opposed to internal data) and their provision of an allegedly more accurate and efficient process, these arguments also fail. Simply limiting an abstract idea, such as the collection of information, to a particular context does not transform the idea into a nonabstract one. *See Elec. Power Grp.*, 830 F.3d at 1353 ("[W]e have treated collecting information, including when limited to particular content (which does not change its character as information), as within the realm of abstract ideas."); *Intell. Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1366 (Fed. Cir. 2015) ("An abstract idea does not become nonabstract by limiting the invention to a particular field of use or technological environment."); *see also Symantec*, 838 F.3d at 1315 ("The novelty of any element or steps in a process, or even of the process itself, is of *no relevance* in determining whether the subject matter of a claim falls within the § 101 categories of possibly patentable subject matter.") (cleaned up). Nor does increasing the speed and efficiency of a process. *See Capital One Bank*, 792 F.3d at 1370 (Fed. Cir. 2015) ("merely adding computer functionality to increase the speed or efficiency of the process does not confer patent eligibility on an otherwise abstract idea").

Where the '331, '524, and '976 patents lack essential details regarding implementation of the proposed method, "the focus of the claims is not on such an improvement in computers as

[1] Other courts have similarly declined to apply *Thales* in the manner BitSight urges. *See, e.g.*, *Cambridge Mobile Telematics*, 2023 WL 4850567, at *6 ("In *Thales*, not only was a novel and specific sensor arrangement disclosed, but the claims covered the techniques for enabling the use of the sensors. . . . The Federal Circuit and courts in this District have rejected attempts to apply *Thales* to claims that lack a specific and novel hardware arrangement.") (collecting cases).

tools, but on certain independently abstract ideas that use computers as tools." *Elec. Power Grp.*, 830 F.3d at 1354. As such, these patents fail *Alice* step one.

ii. *Alice* Step Two

Moving to step two of the *Alice* framework, the '331, '524, and '976 patents contain no inventive concept. BitSight claims that the patents recite an inventive concept where they "provide cybersecurity assessments in a completely new way, by collecting externally available data, without permission of the organization." [Doc. No. 49 at 20]. But this is not "sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice*, 573 U.S. at 221. In *Electric Power*, where the asserted claims focused on "enumerating types of information and information sources available within [a] power-grid environment," the Federal Circuit found that "merely selecting information, by content or source, for collection, analysis, and display does nothing significant to differentiate a process from ordinary mental processes, whose implicit exclusion from § 101 undergirds the information-based category of abstract ideas." *Elec. Power Grp.*, 830 F.3d at 1355. Likewise, merely selecting "externally available information" does nothing significant to differentiate the '331, '524, and '976 patent claims from the abstract processes of collection, analysis, and display. Moreover, "a claimed invention's use of the ineligible concept to which it is directed cannot supply the inventive concept that renders the invention 'significantly more' than that ineligible concept." *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1290 (Fed. Cir. 2018). Where the patent claims are directed to the ineligible concept of collecting and analyzing external data, BitSight also cannot assert the collection and analysis of external data as an inventive concept.

2. The ’834 Patent

i. *Alice* Step One

Next with regard to the ’834 patent, the parties dispute whether the claims “recite a specific enough solution to make the asserted technological improvement concrete,” or whether “the ‘improvement’ captured by those claims was recited at such a level of result-oriented generality that those claims amounted to a mere implementation of an abstract idea on a computer.” *Koninklijke KPN N.V. v. Gemalto M2M GmbH*, 942 F.3d 1143, 1152 (Fed. Cir. 2019). I find the latter to be true.

In *Packet Intelligence*, upon which BitSight relies, the Federal Circuit found a non-abstract idea where the claims met a technological challenge unique to computers—i.e., identifying disjointed connection flows in a network environment—and detailed a technological solution “in several steps.” *Packet Intel. LLC v. NetScout Sys., Inc.*, 965 F.3d 1299, 1309 (Fed. Cir. 2020). Specifically, the claims recited improved packet monitors for “examining packets passing through a connection point on a network,” through a “packet acquisition device coupled to the connection point,” an “input buffer memory” coupled to the pack acquisition device, a “parser subsystem coupled to the input buffer memory and including a slicer” which extracts information from a packet and outputs a “parser record,” a “lookup engine” that checks the information against “flow-entry memory,” and a “flow insertion engine” that determines whether the packet matches an entry in a “flow-entry database” and if so updates the entry or creates a new entry. *Id.* at 1304. The Federal Circuit remarked that the claims thus referred “to specific technological features functioning together to provide that granular, nuanced, and useful classification of network traffic, rather than an abstract result.” *Id*. at 1310.

Here, the ’834 patent does not recite a similarly “granular, nuanced, and useful” solution. Claim 1 describes a computer-implemented method of sending passive queries to an entity’s DNS server and receiving information back, eventually resulting in “mapping each IP address to an attribute for the entity.” [Doc. No. 39-6 at 42]. In other words, the claimed method does nothing more than collect information from DNS servers and then map that information to an entity—without detailing how that mapping occurs. While BitSight alleges that the ’834 patent addresses the technological problem of identifying the domain names, servers, and IP addresses associated with an entity, [Doc. No. 39 at ¶ 66], and uses the “result-based functional language” of mapping, the patent “does not sufficiently describe how to achieve [this result] in a non-abstract way.” *Two-Way Media Ltd. v. Comcast Cable Commc'ns, LLC*, 874 F.3d 1329, 1337 (Fed. Cir. 2017). It is “instead directed to a result or effect that itself is the abstract idea and merely invokes generic processes and machinery.” *Id.* (“Claims directed to generalized steps to be performed on a computer using conventional computer activity are not patent eligible.”). The ’834 patent claims are accordingly directed to an abstract idea—again, the collection and analysis of data, with nothing more.

ii. *Alice* Step Two

Despite BitSight’s protests that the ’834 patent details inventive concepts, on its face, claim 1 does not appear to recite anything beyond the sending and receiving of information. While the claim recites *that* this exchange takes place multiple times, it discloses nothing of substance further than that—namely, *how* the exchange would occur. *See, e.g.*, [Doc. No. 50 at 18 (“***it does not say*** how the DNS queries are formulated to obtain the information in an inventive manner, how the DNS servers process the queries to identify the requested information in an inventive manner, nor how the mapping is done in an inventive manner”)]. “That a

computer receives and sends the information over a network—with no further specification—is not even arguably inventive." *buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1355 (Fed. Cir. 2014). For these reasons, the '834 patent does not recite an inventive concept.

3. The '615 Patent

i. *Alice* Step One

Finally, BitSight asserts that the '615 patent claims are directed to patent-eligible subject matter because they provide a specific method for more accurately and efficiently identifying and mapping assets to an entity. [Doc. No. 49 at 26-27; Doc. No. 39 at ¶¶ 69-70]. Claim 84 recites a three-step method comprising: (1) generating a map between technical assets and entity identities, (2) generating graphs of relationships among entities based on their associations with technical assets, and (3) enabling a user to assist in generating the map by presenting the user with data about the entities' technical assets and providing an "interactive tool" for associating the technical assets with entity identities. [Doc. No. 39-5 at 39]. But, as with the '834 patent, missing from this method is any detail regarding how to achieve each step. The claim simply recites that a map is generated, graphs of relationships are generated, and a user is enabled to assist in generating the map; but such "result-based functional language" cannot, without more, support a non-abstract idea. *Two-Way Media Ltd.*, 874 F.3d at 1337 (finding that an asserted claim fails *Alice* step one where "the claim requires the functional results of 'converting,' 'routing,' 'controlling,' 'monitoring,' and 'accumulating records,' but does not sufficiently describe how to achieve these results in a non-abstract way"). The '615 patent is thus directed to nothing more than the abstract ideas of collecting, analyzing, and presenting information, as with the other Asserted Patents. *See, e.g.*, [Doc. No. 46 at 11-12 and n.3 (collecting cases finding

abstract idea where claims recite receiving, processing, and presenting data, including generating maps therefrom)].

Further, the dependent claims do not add anything of substance to how the claimed generating and mapping take place. They recite types of information or sources from which information may be gathered, but they do not provide details on how to perform the claimed step of generating a map. As such, they cannot render the claims non-abstract. *See Elec. Power Grp.*, 830 F.3d at 1353 ("[W]e have treated collecting information, including when limited to particular content (which does not change its character as information), as within the realm of abstract ideas.").

ii. *Alice* Step Two

Nor do the '615 patent claims recite an inventive concept under the second step of *Alice*. BitSight argues that the "combination of elements" of the claims is innovative, "specify[ing] mechanisms to more completely, accurately, and efficiently associate technical assets with an entity," and detailing "what to do ('generat[e] a map'); how to do it, including by specifying what mechanisms to employ, what information to focus on, and how to locate that information; and then what to do so that the a [*sic*] 'a user to assist in the generating of the map.'" [Doc. No. 49 at 28-29]. But the '615 patent claims plainly do not identity mechanisms to associate technical assets with an entity. Nor do they specify how to generate a map. As set forth above, the claims simply recite generic steps for processing abstract information (i.e., "map," "graphs," and "data"), without the details necessary to implement these steps.

Without these specifications, the '615 patent falls in the class of patents which courts have found "broadly and generically claim 'use of the Internet' to perform an abstract business practice (with insignificant added activity)." *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d

1245, 1258 (Fed. Cir. 2014); *see also Two-Way Media*, 874 F.3d at 1339 (finding no inventive concept where claim only recites "generic functional language to achieve . . . purported solutions" and fails to require anything other than conventional computer components "for *how* the desired result is achieved"). And the lack of inventive concept remains the same whether the elements are taken individually or combined as a whole.

For these reasons, BitSight's claims arising from the Asserted Patents are dismissed.

III. FALSE ADVERTISING CLAIMS

A. Legal Standard

Turning to the non-patent claims, BitSight bears the burden of proof in bringing a false advertising claim under the Lanham Act and must demonstrate the following:

> (1) the defendant made a false or misleading description of fact or representation of fact in a commercial advertisement about [its] own or another's product; (2) the misrepresentation is material, in that it is likely to influence the purchasing decision; (3) the misrepresentation actually deceives or has the tendency to deceive a substantial segment of its audience; (4) the defendant placed the false or misleading statement in interstate commerce; and (5) the plaintiff has been or is likely to be injured as a result of the misrepresentation, either by direct diversion of sales or by a lessening of goodwill associated with its products.

Azurity Pharms., Inc. v. Edge Pharma, LLC, 45 F.4th 479, 486 (1st Cir. 2022) (citing *Cashmere & Camel Hair Mfrs. Inst. v. Saks Fifth Ave.*, 284 F.3d 302, 310-11 (1st Cir. 2002)). Black Kite primarily challenges the sufficiency of BitSight's allegations with regard to the first element, requiring Black Kite to have made "a false or misleading description of fact or representation of fact." *Id.*; [Doc. No. 46 at 33].

This first element requires the subject advertisement to be "literally false or implicitly false." *Cashmere*, 284 F.3d at 311. Literal falsity requires a determination that (1) a claim is conveyed by an advertisement and (2) is false. *Clorox Co. Puerto Rico v. Proctor & Gamble Com. Co.*, 228 F.3d 24, 34 (1st Cir. 2000). While "exaggerated advertising, blustering and

boasting upon which no reasonable buyer would rely" (i.e., puffery) is not actionable, "specific and measurable claims of product superiority" are not puffery and may constitute literally false statements. *Ferring Pharms. Inc. v. Braintree Lab., Inc.*, 38 F.Supp.3d 169, 177 (D. Mass. 2014) (quoting *Clorox*, 228 F.3d at 38-39). Literal falsity is a question of fact. *Id*. Thus, "[u]nless the complained of speech is such that a court can properly say that no reasonable person could be misled by the advertisement in question, . . . it is not appropriate to resolve the issue of the truthfulness of the speech on a motion to dismiss." *Genzyme Corp. v. Shire Hum. Genetic Therapies, Inc.*, 906 F. Supp. 2d 9, 17 (D. Mass. 2012) (cleaned up); *see also Ferring Pharms.*, 38 F.Supp.3d at 177 ("[C]laims of literal falsity will generally survive a motion to dismiss.").

If the advertisement is literally false, then a violation of the Lanham Act may be established "without evidence of consumer deception." *Cashmere*, 284 F.3d at 311. If the advertisement is implicitly false—meaning it is "true or ambiguous but misleading"—then the plaintiff must further prove that the advertisement "conveys a misleading message to the viewing public." *Id.* (citing *Clorox*, 228 F.3d at 33).

B. Analysis

BitSight's false advertising claims may proceed because they involve questions of fact that cannot be satisfactorily undertaken on a motion to dismiss.[2]

"Partial" Integrations and Discovery. BitSight has plausibly stated a claim that Black Kite's statements are false regarding its "extensive" integrations and discovery versus BitSight's "partial" integrations and discovery. Black Kite asserts that claims of extensive and partial integrations and discovery are opinions that cannot be proven, thus constituting mere puffery. [Doc. No. 50 at 19]. But where Black Kite identified allegedly "partial" integrations with

[2] To the extent that BitSight pleads establishment claims in the alternative, [Doc. No. 49 at 31 n.7], I need not reach these claims where BitSight states plausible claims for literal falsity.

specific third parties, in comparison to Black Kite's allegedly "extensive" integrations with the same parties, [Doc. No. 39 at ¶¶ 99-100], a factfinder could reasonably conclude that the Black Kite Comparison claims that Black Kite offers superior integrations as compared to BitSight. Accordingly, BitSight's claim regarding integrations amounts to "a claim in which the advertiser suggests that an attribute, if not measurable, is comparable," such that it may proceed. *Azurity Pharms.*, 45 F.4th at 505; *see, e.g.*, *Clorox*, 228 F.3d at 38-39 (finding "Compare with your detergent . . . Whiter is not possible" advertisements were specific and measurable claims, not puffery, because they invited product comparisons); *Ferring Pharms.*, 38 F. Supp. 3d at 178 (finding that a claim that a drug had "superior cleansing efficacy" was not mere puffery). The same superiority claim applies to Black Kite's statement regarding its "extensive" discovery as compared to BitSight's "partial" discovery, in addition to BitSight's unrebutted argument that "Black Kite's claim is specific and verifiable—a process either traces all data or it does not." [Doc. No. 49 at 34].

Controls. Black Kite argues that "[n]o reasonable consumer would believe Black Kite's webpage conveys anything other than its view of what qualifies as a 'control.'" [Doc. No. 46 at 34]. I do not agree. While Black Kite does provide its distinct definition of "control" elsewhere on its website, this definition is not linked or referenced in the Black Kite Comparison where Black Kite asserts it has 390 controls as compared to BitSight's 40 controls. There is no basis to conclude that a reasonable consumer would have knowledge of this definition. As "a claim concerning a specifically measurable attribute," *Azurity Pharms.*, 45 F.4th at 505, BitSight's false advertising claim regarding each party's number of controls may proceed.

"Instant" New Vendors. Black Kite's assertion that it can add a new vendor "instant[ly]," in comparison to BitSight's allegedly taking "days" to do the same action, again

constitutes a specific and measurable claim of product superiority. Though Black Kite relies on the Central Division of California's decision in *Clark v. Am. Honda Motor Co.*, where the court found a statement that the defendant's product "instantly" factors data in was puffery, that statement was analyzed in the context of an express warranty claim and did not contain a comparison suggesting superiority over plaintiff's product—unlike Black Kite's statement. 528 F. Supp. 3d 1108, 1119 (C.D. Cal. 2021). As to the footnote elaborating that BitSight's "days" actually means, "Days if not pre-evaluated. Instant if pre-evaluated.", [Doc. No. 39-14 at 5], no disclaimer appears next to Black Kite's "instant" claim. A rational factfinder could thus conclude that Black Kite "make[s] a superiority claim either explicitly or by necessary implication," through its comparison of Black Kite and BitSight's time to add new vendors. *Clorox*, 228 F.3d at 35.

Ransomware. BitSight concedes that it does not offer the "Ransomware Susceptibility Index®," as this is the name of Black Kite's branded ransomware likelihood indicator. [Doc. No. 39 at ¶ 107]. Nevertheless, BitSight challenges this statement as it appears on the Black Kite Comparison on the basis that it "misleadingly suggests that BitSight does not offer *any* ransomware likelihood indicator." [Doc. No. 49 at 35]. While "Ransomware Susceptibility Index" may be a trademarked name, the phrase also states the generic service provided—i.e., an index to measure an entity's ransomware susceptibility. And where the comparison appears on a list of comparisons of various other generic services, it cannot be said at the current stage that "no reasonable person could be misled by the advertisement in question" to believe that BitSight does not offer any ransomware likelihood indicator of its own. *Genzyme Corp.*, 906 F. Supp. 2d at 17.

Questionnaires and Attestations. As an initial matter, it is unclear what BitSight means in pleading that "Black Kite has stated in commerce that Black Kite's offerings can have questionnaires and *other security attestations* added but BitSight's cannot," and "BitSight's offerings can, in fact, have questionnaires and *other security attestations* added." [Doc. No. 39 at ¶¶ 110-11 (emphasis added)]. In its Opposition, BitSight references only "security attestations such as questionnaires and custom questionnaire mapping." [Doc. No. 49 at 34]. And the Black Kite Comparison does not make any mention of "security attestations" specifically. [Doc. No. 39-14]. Where the Black Kite Comparison clearly states that Black Kite offers a "Custom questionnaire mapping" and a "Universal Questionnaire and Policy Processor" but that BitSight does not, and BitSight alleges that it does offer questionnaires and custom questionnaire mapping, BitSight's false advertising claim may proceed as to Black Kite's statements on these questionnaires. But the claim is limited as such and shall not reach any claim by BitSight that rests on undefined and unreferenced "other security attestations."

Separately but relatedly, Black Kite argues that BitSight's false advertising claims should be dismissed because BitSight fails to plead any facts supporting its allegations of harm. Under the Lanham Act, "the aggrieved party must demonstrate that the false advertisement actually harmed its business. A precise showing is not required, and a diversion of sales, for example, would suffice." *Cashmere*, 284 F.3d at 318; *see also Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 138 (2014) ("[D]iversion of sales to a direct competitor [is] the paradigmatic direct injury from false advertising."). BitSight pleaded that Black Kite's allegedly false and misleading statements were communicated directly to BitSight's customers by Black Kite salespersons, resulting in "a number of customers who have either switched from BitSight to Black Kite and/or elected to purchase cyber risk management solutions from Black Kite

instead of BitSight." [Doc. No. 39 at ¶¶ 117-18]; *see also* [*id.* at ¶¶ 171-73]. Black Kite's reliance on *Clemente Properties, Inc. v. Pierluisi Urrutia* is misplaced, where the complaint there stated "no more than that [the plaintiffs] have been harmed from the alleged violation of the statute" and did not allege diversion of sales. 693 F. Supp. 3d 215, 246 (D.P.R. 2023). Here, BitSight's allegations pass the threshold to plead harm relative to its false advertising claims.

State law claims "under Mass. Gen. L. chapters 93A and chapter 266, § 91 . . . rise and fall on the merits of the Lanham Act claims." *Euro-Pro Operating LLC v. TTI Floor Care N. Am.*, No. 12-cv-10568, 2012 WL 2865793, at *3 (D. Mass. July 11, 2012). Thus, where BitSight's false advertising claims under the Lanham Act survive, so do its state law claims.

IV. CONCLUSION

For the foregoing reasons, Black Kite's Motion to Dismiss is GRANTED in part and DENIED in part. It is granted as to BitSight's patent infringement claims, Counts 1 through 5. It is denied as to BitSight's false advertising claims and related state law claims, Counts 6 through 8, excluding any claim resting on "other security attestations" beyond questionnaires and custom questionnaire mapping.

SO ORDERED.

/s/ Myong J. Joun
United States District Judge